Carnegie Mellon
Software Engineering Institute

# Information Asset Profiling

**Author**
James F. Stevens

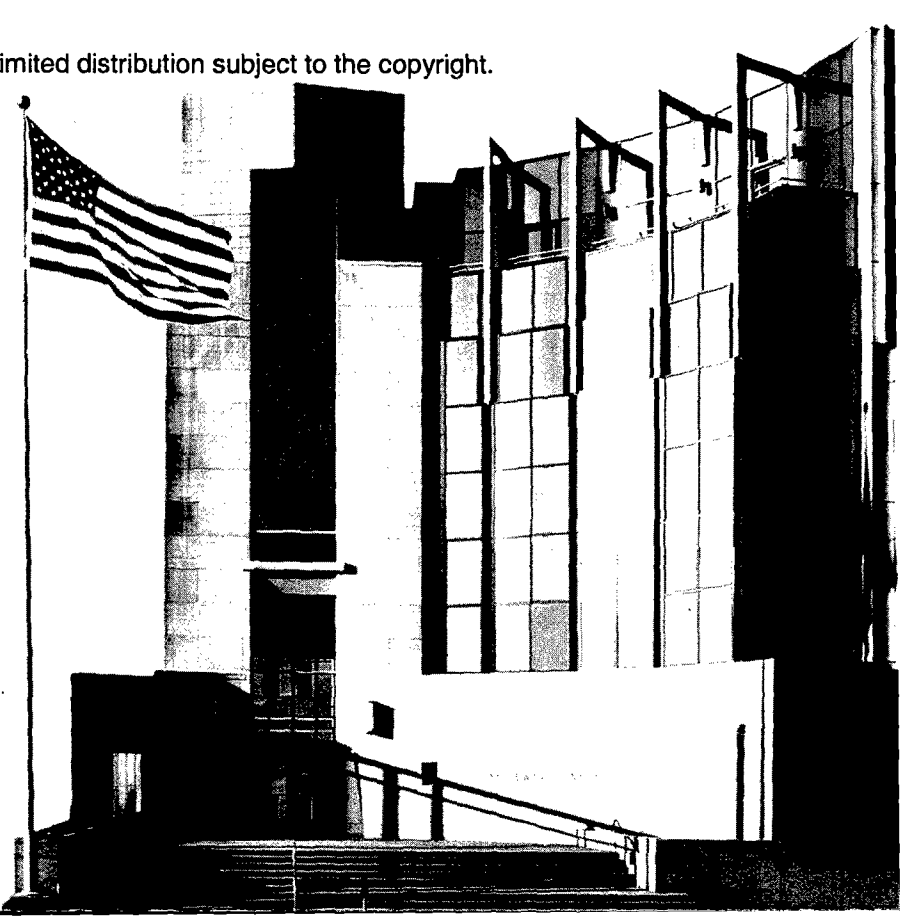
**Principal Contributors**
Richard A. Caralli
Bradford J. Willke

*June 2005*

**Networked Systems Survivability Program**



**Technical Note**
CMU/SEI-2005-TN-021



# Information Asset Profiling

**Author**
James F. Stevens

**Principal Contributors**
Richard A. Caralli
Bradford J. Willke

*June 2005*

**Networked Systems Survivability Program**



**Technical Note**
CMU/SEI-2005-TN-021

This work is sponsored by the U.S. Department of Defense.

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.



This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

# Contents

# List of Figures

# List of Tables

# Acknowledgements

The author would like to thank members of the Survivable Enterprise Management team of the Networked Systems Survivability Program who helped in the production of this report by supplying their ideas, providing content, sharing their experiences in fieldwork with customers, and reviewing drafts. Richard Caralli is the originator of many of the concepts discussed in this document. Bradford Willke created much of the example materials included in the appendix and contributed significantly to the codification of the IAP process. We would also like to thank the General Services Administration's Integrated Acquisitions Environment for the opportunity to develop the initial concepts behind the IAP process.

We are also grateful to David Biber for his extensive work in creating the wonderful graphics that appear throughout and to Pamela Curtis for her careful editing of this report. We would also like to thank William Wilson, William Fithen, and Derek Gabbard for reviewing and providing feedback on the document.

Last, but not least, we would also like to thank our sponsors for their continued support of this work. We believe that it will help organizations begin to more effectively and efficiently address their information security risks.

# Abstract

The steadily increasing technical and environmental complexity of today's globally networked economy presents many obstacles to organizations as they attempt to protect their information assets. Information assets are constantly processed and combined to form new information assets. The line between ownership and custodianship of information assets blurs as information freely flows throughout an organization and often crosses outside organizational boundaries to other entities such as partners, customers, and suppliers. The CERT Survivable Enterprise Management group at the Software Engineering Institute developed the Information Asset Profiling (IAP) process as a tool to help organizations begin to address these security challenges.

The authors describe IAP, a documented and repeatable process for developing consistent asset profiles. They also explain how the development of an information asset inventory using the IAP process provides a strong basis for organizations to begin to identify and address their information security needs.

# 1 Introduction

The steadily increasing technical and environmental complexity of today's globally networked economy presents many obstacles to organizations as they attempt to protect their information assets.[1] Information assets are constantly processed and combined to form new information assets. The line between ownership and custodianship of information assets blurs as information freely flows throughout an organization and often crosses outside organizational boundaries to other entities such as partners, customers, and suppliers. The CERT Survivable Enterprise Management team developed the Information Asset Profiling (IAP) process as a tool to help organizations begin to address these security challenges.

## 1.1 IAP Process Overview

The IAP process provides an organization with

- common, consistent, and unambiguous understanding of information asset boundaries
- clearly designated asset owner or owners
- a complete set of information security requirements for each asset
- descriptions of where the asset is stored, transported, and processed
- an opportunity to determine the asset's value

The ultimate goal of the IAP process is to provide a common definition of an information asset that all stakeholders can utilize when developing and applying a protection strategy and risk mitigation plans for that asset. Accurate asset definitions help in the selection of controls to protect an asset. If this information is introduced early in the system development life cycle, controls can be designed to ensure that the security requirements of an asset are enforced. Asset profiles can also provide context and meaning to compliance and audit activities—management can make informed decisions on how to respond to these findings by referring to security requirements and the asset's value.

In addition to supporting the information security risk management process, the development and communication of information asset profiles can help to develop more secure business processes. By being aware of the explicit security requirements of an information asset, organizations are able to make more informed decisions and can adjust or improve business processes accordingly.

[1] Information assets can be described as information or data that is of value to the organization, such as patient records, intellectual property, or customer information.

The IAP process is an iterative one and has been broken into six distinct activities (see Figure 1). Each activity in the process captures additional information about an information asset, and this information may alter an organization's perception of that asset. For example, an organization may determine that it makes more sense to consider an asset as two separate information assets instead of one very large asset. When this happens, the process should be restarted with each asset to ensure consistency and accuracy.

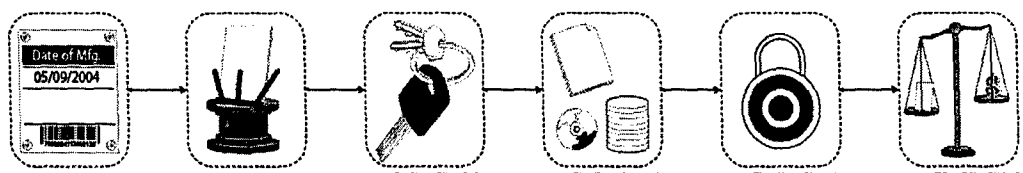



*Figure 1: The IAP Process*

The profiles created by the IAP process are meant to be living documents within an organization. As the organization evolves and changes, so do its information assets. Thus corresponding asset profiles may need to be updated and new profiles created as new assets are identified. The idea of asset profiling is to capture just enough information so that the profile produced by the process is useful but not cumbersome to manage and change.

## 1.2 To The Reader

The rest of this report describes how information asset profiles can help organizations address many of the security issues in today's networked environments.

Section 2 describes how asset profiling helps organizations confront many information security challenges.

Section 3 looks at the complex relationships between information assets, owners, and custodians and how the profiling process can provide clarity.

Section 4 provides a brief overview of how information asset profiles could be used to drive information security risk assessment activities, essentially a list of possible next steps for an organization that has used the IAP process to inventory its assets.

Section 5 describes future directions for the IAP process and other related work.

Appendix A contains a detailed guide to the IAP process and examples to be used by organizations wishing to develop their own information asset profiles. While this information can act as a standalone guide to the process, it is recommended that the body of this report be understood before attempting to use the IAP process in an organization. It provides a common vocabulary and conceptual representation of the goals of the process.

Appendix B contains IAP worksheets that organizations can use to create their own information asset profiles.

# 2 IAP and Information Security

The IAP process was designed to help organizations confront a number of information security challenges. These challenges and how developing an inventory of asset profiles can address them are discussed in the following sections.

## 2.1 Information Asset Boundaries

Data is factual information used for the purpose of reasoning, discussion, or calculation [Webster 04]. Information is the communication or reception of knowledge or intelligence [Webster 04]. For our purposes, data is simply a subset and essential component of information. The transformation of data into information occurs because organizations use raw data typically in the aggregate and within a given context, yielding the business information and intelligence.

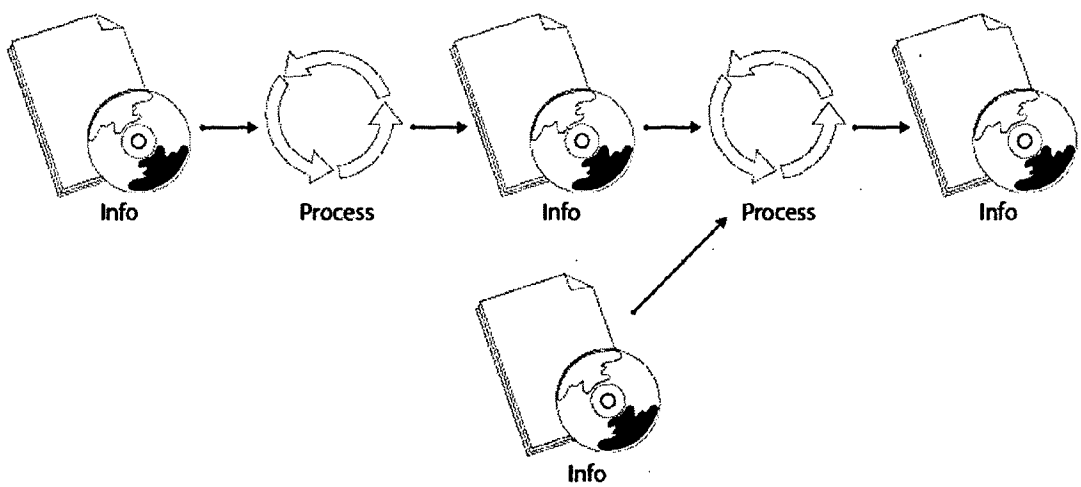



*Figure 2: The Information Cycle*

The continual cycle of moving data through a process that creates information (see Figure 2) results in challenges for determining the boundaries of an information asset. For example, data from two different sources is sometimes combined to create a new information asset. For security purposes, this poses several questions:

- Is the new information asset substantially different from the assets that it was derived from? (Thus, is it truly a new information asset?)
- Who is the owner of the new asset? Is it one of the owners of the two assets from which it was derived, or is it an entirely new owner?

- What are the security requirements for the new asset? Are they simply the combination of the security requirements of the two assets from which the new asset was derived, or an entirely new set? Are the security requirements for the new information asset more or less extensive than those of one or both of the assets from which it was derived?

The development of asset profiles using the IAP process allows an organization to address each of these security questions. By creating *consistent, unambiguous, and agreed upon* definitions for its information assets, an organization determines whether new information generated by a process is in fact a new asset. Once an asset is bounded, an organization can determine not only uniqueness but also ownership and security requirements. A clear boundary on the asset is also required for determining an asset's value. The value of an asset to an organization can only be determined if the person or persons responsible for that process understand and agree on exactly what is being evaluated.

## 2.2 Identifying Asset Containers

The place where an information asset "lives" can be termed a *container*. Generally, a container describes some type of technology asset—hardware, software, or an information system—but it can also describe people, paper, or CD-ROMs. Therefore, a container is any type of asset where an information asset is stored, transported, or processed. It can be a single technology asset (such as a server), a collection of technology assets (such as an information system or a network), or a person who has knowledge of an information asset (such as the case where one particular employee in the organization knows the confidential designs for the widgets), or simply a piece of paper with information printed on it.

There are three very important points with respect to security and the concept of an asset container:

- The way in which an information asset is protected or secured is through controls implemented at the asset container level. For example, to protect the customer database on a server, a layered collection of controls (administrative, physical, and technical) are applied to the server, such as only permitting authorized individuals to enter the server room (a physical control) and limiting access to administrative permissions on the server to system administrators (a technical control).
- The degree to which an information asset is protected or secured is based on how well the implemented controls, at the container, align with and consider the security requirements (or objectives) of the asset. This is different from simply implementing the available or standard set of controls offered by the container, which may arbitrarily protect the information assets it supports.
- Any risks to the containers on which the information asset lives are inherited by the information asset. Thus, when determining risks to the information asset, the vulnerabilities of the container must be considered. For example, if an information asset is stored on a server that is in a room that does not limit access, it is vulnerable to disclosure, modification, loss, or destruction by an actor using physical access. The value

of the server in this case is probably negligible—it can be replaced quickly or its function can be moved to another server—however, the information asset stored on the container is not as easily replicated if compromised, and the impact to the organization is much more extensive.

The type of container in which an information asset resides can often have significant effects on the security requirements and protection strategies of an asset. There are many laws and regulations that require information assets to be protected in specific ways depending on the format in which they are stored. There are often different regulations for paper and electronic records; in some cases, regulations exist for information assets stored in one type of container, while no regulations exist for other container types.

By capturing the security requirements and mapping an information asset to each of its containers, the IAP process provides critical information to an organization's information security decision makers. At the container level, decisions can be made as to what system of controls needs to be applied by the container to protect the information asset. For example, if the container is a piece of paper, then perhaps an administrative control that states that the asset must be locked in a filing cabinet when not in use would be applied. Mapping an asset to all of the containers on which resides efficiently bounds the control environment required to secure that asset.

Finally, every control has a cost. Having a sense of value for an information asset provides additional information to the development of a protection strategy of the asset. Organizations can use the value information captured in the asset profile to begin to determine whether implementing a control is worth the cost. This allows an organization to make more informed risk management decisions.

## 2.3 Owners and Custodians

The owners of an information asset are those individuals who have primary responsibility for the viability and survivability of the asset. The term "custodian" refers to any individual in the organization who has the responsibility to protect an information asset as it is stored, transported, or processed.

### 2.3.1 Owners of Information Assets

Owners set the security requirements for information assets and are responsible for communicating those requirements to all of the assets' custodians. Owners are also responsible for periodically determining that the security requirements for their assets have been implemented through a layered control approach and that the controls in fact meet the security requirements.

In addition to setting security requirements, owners of information assets are responsible for two other important tasks:[2]

- Owners are responsible for setting the definition and the scope of an information asset. Often, the boundaries of an information asset are not clear—for example, the information asset "customer data" is somewhat vague because it lacks definitive boundaries. Thus, it is the responsibility of the owner of the asset to develop a definition of the asset that can be consistently applied by custodians and users of the asset as well.
- Owners are also responsible for understanding the value (monetary or otherwise) of the asset to the organization. The value of an asset determines its importance and criticality to the organization. The value of an asset drives the development of an appropriate risk mitigation strategy. For example, management should only support risk mitigation strategies that cost less than the value of the asset or the impact on the organization if the asset is destroyed or compromised.

An owner may delegate these security responsibilities, but the owner remains ultimately responsible for the protection of the asset. Unfortunately, in many organizations the owners of information assets are unaware of their responsibilities. The IAP process compels an organization to identify who has ownership responsibility for a given information asset. Once owners are clearly identified, the organization can begin to require the owners to fulfill their security obligations for that asset.

### 2.3.2 Custodians of Information Assets

In essence, custodians manage or are responsible for containers. The term custodian implies a custodial relationship between the custodian and the information asset. Thus, when the information asset is in the hands of the custodian to manage (i.e., it is on a server or information system that the custodian administers), the custodian accepts responsibility for the asset and ensures that it is protected. In many organizations this accepting of responsibility to protect the asset is mistaken for ownership.

The custodian concept is most typically considered in terms of information technology administrators and managers who take custodianship of information assets as a part of their responsibilities for supporting the business functions of the organization. However, custodial responsibility for information assets exists in many additional circumstances. For example, users take custodial control of assets as they use these assets in carrying out the daily operations of an organization. Any technology or person who ultimately stores, processes, or transmits an information asset for any duration of time or purpose is a container, and whoever manages that container has custodial responsibilities for that asset (see Figure 3).

[2] Collectively, these two tasks represent an owner's responsibility to perform information asset profiling.

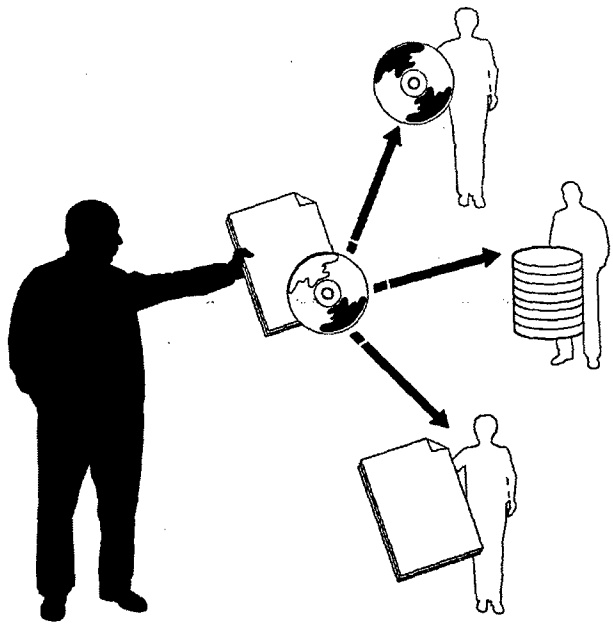


*Figure 3: Custodial Responsibilities Exist in Many Circumstances*

As an example of this, consider an organization's customer database as an information asset. The security requirements for the asset have been developed by the owners and have been implemented through controls applied at the server (container) level by custodians. Under the custodial control of the information technology (IT) department, the asset is adequately protected. However, suppose a user has access rights that allow her to download a portion of the customer database to her desktop to perform trend analysis. The information asset (or a portion of it) now resides on a new container. In essence, the user, as the manager of that desktop, is temporarily also a custodian. Custodians are generally required to provide due care over the information asset while it is in their possession. Thus, the user should ensure that she protects this information asset as well as or better than it was protected at the container from which she received it. More importantly, the user should protect the information asset commensurate with its security requirements. If she cannot, the owner of the information asset should deny her access to it or deny her the privilege of acting as a custodian for the information.

Users do not have custodial responsibilities only when they make a copy of a database. By having information in their heads, they are containers for the information asset and have a responsibility to protect it accordingly. The same can be said when an administrator makes a backup copy of a database and hands it to another individual who manages tapes. The tape manager now has a custodial responsibility for that information asset. The challenge with protecting an asset is to ensure that, first, security requirements and responsibilities are communicated to all custodians who have access to an information asset and, second, that they are able to implement appropriate controls to meet those requirements.

There are three important points regarding the relationship between custodians and information assets:

- Custodians are responsible for implementing the security controls at the container level that protect an information asset. Owners also often delegate, either implicitly or explicitly, the responsibility of selecting controls to a custodian. However, the owner is still responsible for ensuring that the controls are adequate. The appropriate controls should be based on the security requirements for the information asset and are set by the owner of the asset. The custodian is responsible for implementing a level of controls commensurate with the security requirements set by owners when taking custodianship of an information asset. Implementing appropriate security controls requires knowing the security requirements. The IAP process captures this information for a given asset. These requirements can be then shared with all of the custodians of that asset.
- Custodians are often involved in educating the owner on the availability and options of security controls. In this manner, the custodian(s) and owner can have conversations about the appropriateness of controls in meeting the owner's security and operational requirements. For these conversations to take place, the owner must understand who the custodians of an information asset are and the custodians must understand the security requirements of that asset.
- Custodians often have a difficult job because there is frequent commingling of information assets on a single container or across multiple containers. Thus, the custodian is challenged to meet the sometimes different security requirements of two or more information assets that live on the same technology assets. This specific situation is addressed in the next section of this document.

# 3 Managing Information Assets

The roles and responsibilities of both owners and custodians should be explicitly defined and understood throughout the organization.

## 3.1 Owners and Custodians

Owners direct custodians to implement security controls commensurate with the security needs of an information asset. Thus the job of planning and managing security is the responsibility of owners and custodians jointly. Unfortunately, in many organizations this is not the case. The owner and custodian concepts create complex situations for managing the security of an information asset and for performing information security risk management activities. It is important to understand some of the potential scenarios—referred to as *dilemmas of data*—and understand how information asset profiles can help organizations address these dilemmas.

### 3.1.1 Information Asset Owner and Custodian Are the Same

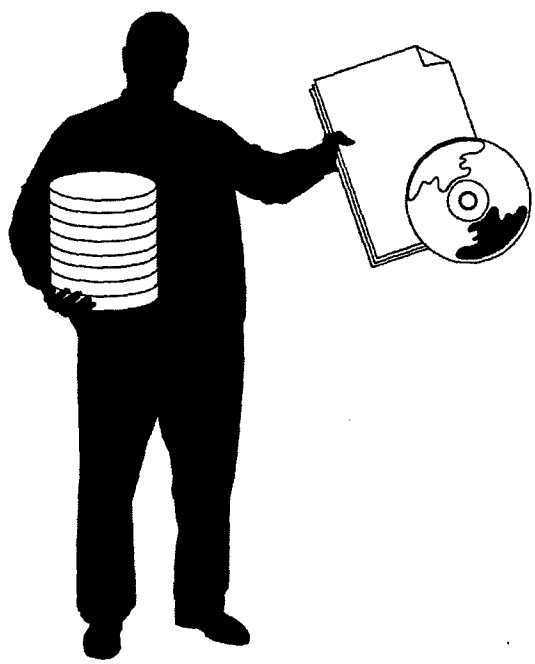


*Figure 4: Owner and Custodian Are the Same*

In some cases, the owner of the information asset is also the owner of the technology assets and environment in which the asset lives (see Figure 4). When this is the case, the owner of

the asset is responsible for implementing the controls at the container level that are commensurate with the security requirements the owner has set for the asset.

### 3.1.2 Information Asset Owner and Custodian Are Different

A more likely scenario is the situation where the owner of an information asset and the custodian of the asset are different (see Figure 5). In this case, the owner is responsible for determining the security requirements of the asset (based on its value) and communicating them to the custodian. In turn, the custodian is responsible for meeting the requirements by implementing appropriate controls on the containers where the asset is stored, transported, and processed.

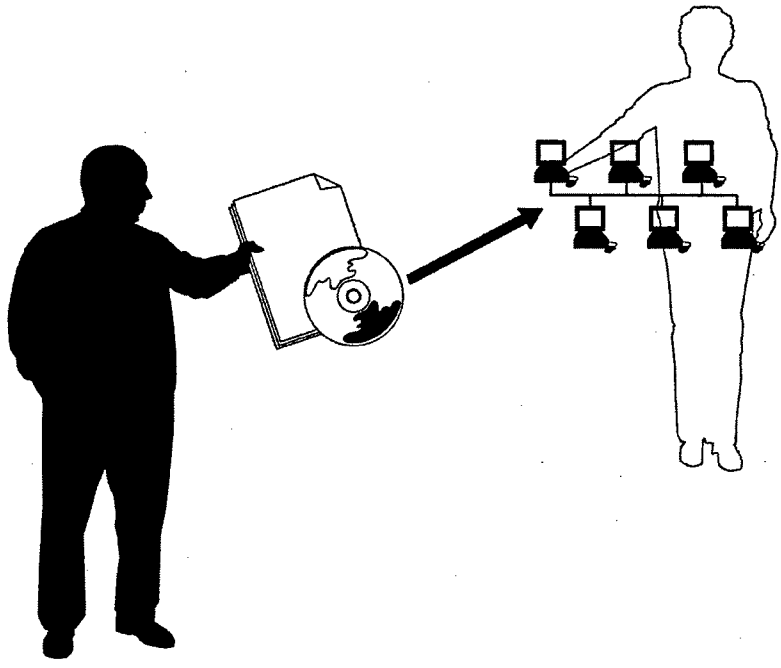


*Figure 5: Owner and Custodian Are Different*

The collaboration between business experts and information technology highlights the scenario in which the owner of an information asset is different from the custodian. Frequently, the true owners of information assets are the business subject matter experts who entrust the IT department to manage their technical infrastructure. Unfortunately, these owners are often unaware of their role and abdicate their responsibilities to the custodians of their data. Thus, they relinquish all control of the asset to the IT department and expect them to manage all aspects of the asset, including security.

As the administrators over information system and technical infrastructure, the IT department takes on the job of supporting the business functions of the organization. Since the business functions of the organization are dependent on information assets, the IT department plays an important role in implementing protection strategies that support and protect the organization's information assets. The criticality of their role and their ability to implement

technical controls has led many organizations to mistakenly attribute ownership of information assets to them.

Sometimes, the owner of the asset is also the owner of the technology assets and environment, but does not directly manage this environment. For example, an asset owner may contract the management of the environment to an outside contractor. Even though the asset owner also owns and is responsible for the container, he or she must still communicate the security requirements to the outside party that is acting as the agent for custodianship and must ensure that the requirements are being met through an appropriate layer of controls.

### 3.1.3 Many Different Assets, Owners, and Custodians

In the real world, the most prevalent scenario is one in which a custodian (such as the IT department) is managing a container or containers on which many different information assets are stored, transported, and processed (see Figure 6). A further complication is that each of the information assets may have different owners and, consequently, potentially different security requirements. Traditionally, this scenario sets up the condition where IT personnel by default set the security requirements for the technology asset without regard to the information assets and their owners. In their defense, most IT personnel are not provided direct instruction on the security requirements for the individual assets; therefore, they apply a general strategy that aims to protect all of the assets.

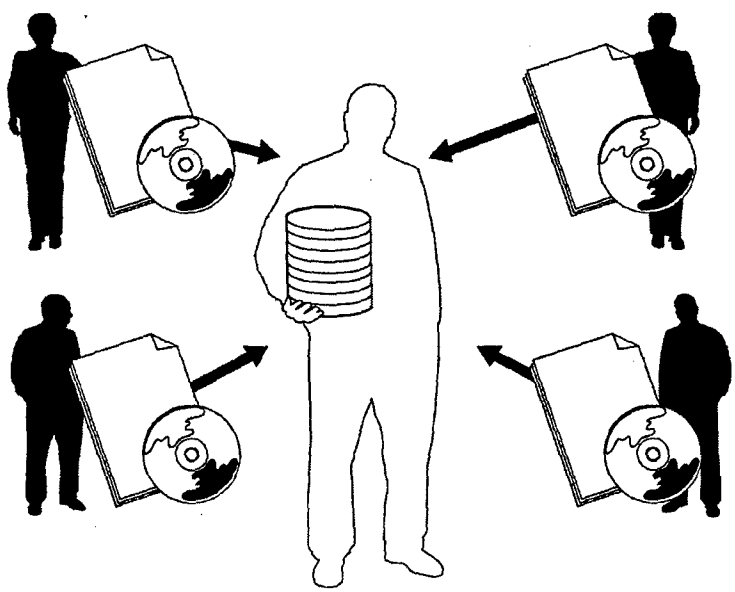


*Figure 6: Many Information Assets on the Same Container*

While this is effective in some situations, it usually exposes some information assets to vulnerabilities and risks that should and could be mitigated with the implementation of a proper level of controls. This is a challenge, however, because the minimum level of controls on the container must be those that meet the highest level of security requirements needed to

secure one or more of the information assets. In other words, the information asset with the most extensive security requirements influences the overall controls applied to the container.

A common consequence of this situation is that some assets on a container will be over-protected because the controls are more extensive than is called for in their security requirements. Most often, however, the controls applied to a container end up failing to accurately reflect the security needs of all the information assets it stores, processes, or transports. Frequently, this results in moving information assets to other containers (e.g., servers) where they can be protected in a way that better meets their security requirements. Organizations are often ill-equipped or unaware of the need to do this, however, or are unwilling to due to the potential increase in cost, and therefore do not act.

## 3.2 IAP and Dilemmas of Data

Each of the dilemmas of data adds a layer of complexity in protecting an organization's information security assets. Developing an inventory of all an organization's information assets using the IAP process

- bounds the assets
- identifies owners
- identifies security requirements
- maps assets to containers
- values the asset

Mapping an information asset to all of its more critical containers leads an organization to the technology assets, physical records, and people that are important to storing, transporting, and processing the asset. That information can also be used to determine all of the information assets that live on a specific container. The assets on that container can then be considered collectively when developing a system of controls to implement on that container. In some cases an organization may determine that allowing certain combinations of assets to coexist prevents the development of an efficient system of controls, and an owner may choose to prevent an asset from existing on a container. By capturing the value of an information asset, the profiling process provides necessary information for an organization to consider cost benefit tradeoffs when designing a protection strategy. Finally, the identification of owners, security requirements, and container managers allows an organization to ensure that the stakeholders can be involved in the decision making.

# 4 Next Steps For Asset Profiles

This section of the report is not intended to describe a detailed process for conducting an information security risk assessment; rather, we intended it to describe how the information in an individual information asset profile or inventory of profiles can be applied to information security activities.

## 4.1 IAP and Risk Assessment

Achieving long-term success requires that organizations make efficient and effective choices in deploying their limited resources (personnel, time, and money). Unfortunately, many organizations are unsure how or even where to deploy their scarce resources in protection of their information assets. The steadily increasing technical and environmental complexity of today's globally networked economy presents a significant obstacle in efficient deployment of resources. Adding to the complexity is the growing list of information security vulnerabilities and threats to which organizations are continually subjected.

In the face of this complexity many organizations choose to spend their resources identifying and managing information security vulnerabilities instead of managing risk to their information assets. Vulnerability-centric approaches to organizational security fall short of appropriately characterizing organizational risk because they fail to focus on what is actually at risk, the information and processes they support. The existence of a significant vulnerability does not mean that an organization is at a significant risk. A vulnerability is only significant if it places a critical asset at risk. This is an important distinction because assets and their value to the organization determine the context for risk rather than the vulnerability itself.[3]

The process of creating information asset profiles as described in this report helps an organization to develop an inventory of its information assets and to describe those assets in sufficient detail to convey their value to the organization. The value of the assets can then be used to determine their criticality. The identification of critical information assets is the first step in performing an information security risk assessment.[4] Collectively, these assets define what is important to the organization and must be protected.

[3] The importance of considering vulnerabilities in an organizational context is recognized in the Common Vulnerability Scoring System (CVSS), which was recently proposed by the National Infrastructure Advisory Council (NIAC). The scoring system includes an organizational component that rates the vulnerability according to each organization's unique context.

[4] A critical information asset is an asset that is essential to an organization's being able to achieve its mission.

Techniques such as the critical success factors methodology can be used to align the asset valuation process with the strategic drivers of the organization, providing the necessary context for information security risk evaluation [Caralli 04]. In the federal space, a significant amount of guidance has been issued to help federal government agencies determine a valuation for their information assets. FIPS Publication 199 [NIST 04a] and the NIST Special Publication 800-60 volumes [NIST 04b] provide explicit guidance.

Once information asset profiles have been completed for critical information assets, the organization can begin the process of identifying risks to those assets and planning strategies to mitigate the risks. A typical information security risk assessment consists of several major activities:

- characterizing risks (from vulnerabilities and threats)
- determining the consequences to the organization if these risks are realized
- evaluating, categorizing, and prioritizing which risks need to be mitigated
- developing corresponding mitigation strategies and plans

Many available commercial and governmental risk assessment methodologies contain these basic activities and can be modified or tailored to accommodate a focus on information assets. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) information security risk assessment methodology [Alberts 01] is one example of such a tool. Another example can be found in NIST Special Publication 800-30, the *Risk Management Guide for Information Technology Systems* [Stoneburner 02]. Using information asset profiling to identify and characterize critical information assets allows an organization some freedom in choosing the risk assessment approach that best suits its particular needs and unique operating circumstances.

## 4.2 Information Asset Driven Risk Assessment

An information security risk assessment is a process of determining the vulnerabilities, threats, and risks[5] to an organization's critical information assets. This process relies on the experience and insight of the organization to determine those risks that most need to be mitigated because they can impede the organization's ability to achieve its goals and accomplish its mission. Information asset profiles document the important characteristics of information assets and thus can be used effectively as the primary focus of an information security risk assessment.

An information asset driven assessment is characterized by the use of information assets as the primary focus and driver for the assessment. Following the trail of an information asset as it traverses the organization (and its external environment) naturally expands the scope and

® OCTAVE is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

5 We use the term "risks" generically in this section to collectively represent information security vulnerabilities, threats, and risks.

reach of the risk assessment to areas that might not otherwise be considered by the organization (see Figure 7).

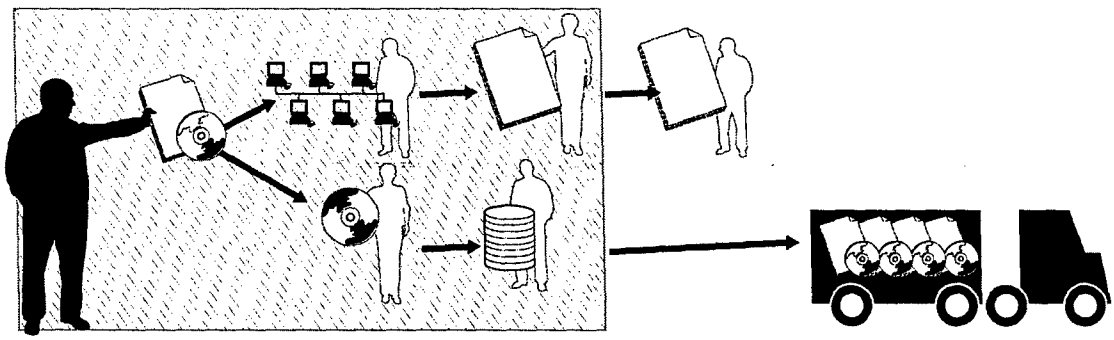


*Figure 7: Following an Information Asset As It Traverses an Organization*

There are three essential elements to performing an information security risk assessment that is focused on information assets:

- determining the information asset's key containers
- identifying vulnerabilities, threats, and risks to the information asset (i.e., issues related to the key containers)
- planning for the mitigation of risks

These elements are described in more detail in the following sections.

### 4.2.1 Key Containers

As described in Section 2.2, a container is any place where an information asset "lives." A key container is simply a container on which a critical asset is stored, transported, or processed.

In an information security risk assessment, the identification of key containers is essential to identifying the risks to an information asset. By mapping an information asset to its key containers, the IAP process defines the boundaries of the technical environment and infrastructure that must be examined for risk.[6] It also provides insight into the types and extent of risks to which the information asset is exposed, specifically allowing potential access paths to be investigated and confirmed.

Another important benefit of identifying key containers for assessment is that it ensures that internal and external risks to an information asset are considered. Information assets are often transported across organizational boundaries, yet traditional risk assessments may focus on vulnerabilities and threats that affect only the key containers that are under the organization's direct control. However, many of the most onerous risks to an information asset fall outside

[6] This is an area where the custodian is instrumental in aiding the owner in understanding the appropriateness of current controls and safeguards, as well as how vulnerabilities and threats expose the asset to undesirable consequences (and impact) or risk.

of these boundaries. Consider the case where an organization outsources the backup and recovery services for one of their important information assets. The service contractor that performs the backup may transport the information asset to a subcontractor under a contractual agreement. The organization that owns the information asset may not be aware of this agreement. By mapping the information asset to its key containers both inside and outside of the organization, the key containers of its contractor, and, in turn, its subcontractors, are included as sources of risks to the information asset as targets of risk mitigation activities.

In addition, this approach to risk assessment considers the influence of people and the risks they present to information assets. A person in the organization can be a key container of an information asset, such as intellectual property. Risks to the availability of this information asset related to the availability of the person must be identified and mitigated.

### 4.2.2 Risk Identification

An information asset driven risk assessment approach is effective at placing information assets in the context of their risk environment. It is nearly impossible to provide an accurate picture of risk without considering the information asset's operating environment. Thus, in many cases, the identification of risks to key containers results in the identification of risks to the information asset as well.

There are three typical areas of risk identification that can be applied at the key container level: technical, physical, and organizational.

- Technical risks are those risks that are inherent in the technical infrastructure in which the information asset lives. These risks can be extracted by analyzing the vulnerabilities in the infrastructure. For example, permitting the use of a "guest" userid may allow unauthorized access to a server, which in turn can allow the information asset on the server to be compromised. Vulnerabilities are typically identified through the use of vulnerability assessment tools that compare the technology asset's (or infrastructure's) configuration against a catalog of known vulnerabilities.
- Physical risks are those risks that result from physical access to an information asset via access to a key container. For example, permitting unauthorized personnel to enter the server room can allow a server to be shut down, impeding the availability of the information asset on the server either temporarily or permanently. These types of risks are generally identified through the identification of various physical access scenarios and an examination of the effectiveness of current physical controls against best practices.
- Administrative risks are those risks that an information asset inherits as a result of organizational or operational weaknesses and vulnerabilities. For example, failure to have an information security policy that is known to all users and administrators can put all of the organization's critical information assets at risk. Administrative risks are generally

identified through an examination of the organization against best practices in the area of organizational and operational controls.

In addition to these traditional layers of risk, other types of risk can be identified by using an information asset driven approach. For example, organizations often do not have a clear one-to-one relationship between information assets and key containers (i.e., the dilemmas of data). Where more than one information asset is present on a key container, the ability to manage security to satisfy each asset's security requirements becomes complex and can be diminished. This poses additional risk to all information assets on that container. By performing an analysis of information assets using a key container context, these types of risks are identified and can be addressed, particularly when developing mitigation strategies.

The ability to identify risk at the key container level, regardless of whether the key container is internal or external to the organization, enables the development of a more robust risk profile for an information asset. It also enables an organization to more fully analyze the potential impact of risk so that a balanced (risk vs. reward) mitigation strategy can be developed.

### 4.2.3 Risk Analysis and Mitigation

Risks are meaningful to the organization only if the risk

- impedes the ability to meet an information asset's security requirements
- results in an undesired consequence to the organization

Analyzing risk requires considerable effort and information to determine whether the risk is such that the organization should act by deploying limited human and monetary resources. Thus, the organization must consider several factors and questions:

- Does the risk impair the value of the information asset and its contribution to meeting the organization's mission?
- Should the risk be mitigated, transferred, or accepted?
- What is the most appropriate and cost effective mitigation strategy for risks that the organization must mitigate?
- Is the cost of mitigation higher than the potential impact to the organization if the risk is realized?
- Does the risk mitigation strategy suggest a layered approach (physical, technical, and administrative) so that all types of risk are considered?
- Does the most cost effective risk strategy (mitigation, transference, or acceptance) result in a level of residual risk that the organization can accept?

Answering these questions for each of the organization's information assets can be difficult. However, the use of an information asset profile provides much of the necessary information, well in advance of risk analysis and mitigation. As a result, the organization can begin

considering these issues while an asset is being profiled rather than only through risk assessment and mitigation activities.

# 5 Future Work

With the IAP process an organization can identify, describe, and build an inventory of its information assets, an important step in attacking the environmental complexity that hinders information security activities. However, we view the IAP process as only one of several first steps in an effort to change organizational approaches to enterprise security. We are currently conducting significant research in the area of enterprise security management.[7]

It is our belief that an information asset centric approach to information security risk management, which starts with building information asset profiles, will focus an organization's information security activities on the information assets and supporting infrastructure that most contribute to the organization. Using information assets as the driver for the asset security risk assessments, as outlined in Section 4, can ensure that the assessment is effectively and efficiently scoped. Over the next few years we expect to explore these concepts in more detail and to develop and transition additional information asset driven risk management techniques.

The readers of this technical note are encouraged to adopt and refine the IAP concepts. Comments, suggestions, and descriptions of your experiences with the process and the templates presented in the following appendices can be directed to the author of this report (jfs@cert.org).

[7] This new direction is described in more detail in the following publications:
*The Challenges of Security Management* at http://www.cert.org/archive/pdf/ESMchallenges.pdf and *Enterprise Security Management: An Executive Perspective* at http://www.cert.org/archive/pdf/ESM.pdf.

# Appendix A IAP Method Description

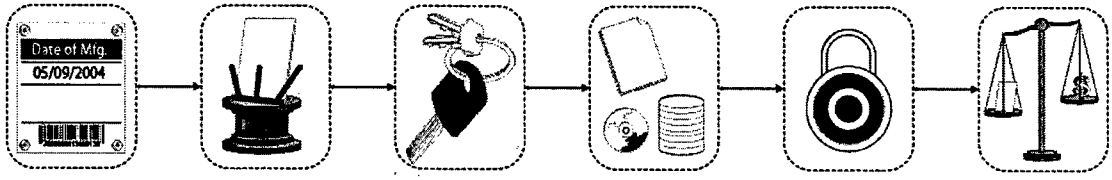
## IAP Process Overview

The Information Asset Profiling (IAP) process is a tool that an organization can use to create consistent, unambiguous, and agreed upon definitions of its information assets. The process also provides a platform upon which organizations can more objectively begin to valuate their information assets. The IAP process provides an organization with

- clearly designated asset owner or owners
- common, consistent, and unambiguous understanding of information asset boundaries
- a complete set of information security requirements for each asset
- descriptions of where the asset is stored, transported, and processed
- an opportunity to determine the asset's value

An information asset profile describes an information asset with enough detail to accurately and consistently characterize it throughout the organization. This does not mean that the information asset must be described in exhaustive detail; rather, it provides a common definition that all stakeholders (owners, custodians, and users) can utilize when developing and applying a protection strategy. The idea is to capture just enough information so that the profile is useful but not cumbersome.

The IAP process has been broken down into six activities:




**ACTIVITY 1** Capture Background Information

**ACTIVITY 2** Define the Information Asset

**ACTIVITY 3** Identify the Asset Owner

**ACTIVITY 4** Identify Containers

**ACTIVITY 5** Identify Security Requirements

**ACTIVITY 6** Determine the Information Asset Valuation

The amount of time taken for each activity is dependent on the complexity of the information asset, the experience of the team developing the profile, and the organizational resources available to the team.

Each of these activities is described in detail in the following sections of this report. Each activity description begins with a purpose statement that defines the primary goal of the

activity. The purpose statement is followed by a concepts section, which provides more details on the motivation for the activity. A collection of tips on completing the activity follows, along with a list of steps for completing the activity. An example information asset profile is developed throughout the exercise to provide additional guidance.

This methodology for capturing information asset profiles is meant to be iterative. At each step in the process the new information captured may alter how decisions would have been made in previous steps. When this happens, the process should be reset to ensure consistency with previous steps. The point of reset is where a different decision would have been made in consideration of the new information learned. Within the description of each activity below, attempts are made to call out typical situations where the need for iteration might arise.

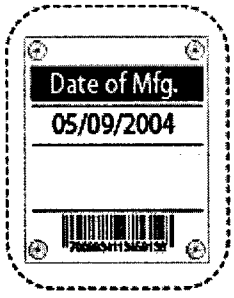
The makeup of the team developing information asset profiles is highly dependent on the complexity of the information asset and the complexity of the organization. It is recommended that the team developing the profile include individuals who will be using the profiles. This helps to ensure that the profiles will meet their usefulness requirements. In addition, it is important to involve the owner of the asset and other relevant stakeholders in the process. This will ensure the accuracy and consistency of the definition and the acceptance of stakeholders. At the very least these individuals should be made available to the team developing the profile.

## IAP Next Steps

The IAP process was designed to be a first step for an organization toward securing its information assets. Once an inventory of information assets has been created through the IAP process, the organization has a wealth of information on which to base additional information security activities. Collectively, this inventory describes what must be protected by the organization. The value of the assets can be used to determine their criticality and drive a risk assessment process. The mapping of assets to containers can bound a vulnerability analysis activity for a given asset. The clear statements of security requirements and mapping to containers can feed the development of a protection strategy for that asset and provide fodder for a control audit.

Finally, the profiles created by the IAP process are meant to be living documents within an organization. As the organization evolves and changes, so do its information assets. As assets evolve, the corresponding profiles need to be updated, and as new assets are created, new profiles need to be created.

## Activity 1 - Capture Background Information




### Purpose

The purpose of this step is to collect information about who is completing the information asset profile and when the profile is being completed.

### Concepts

Information assets are likely to evolve over time; thus, an information asset profile may need to be updated or re-created. Although the information collected here is not directly used in developing information asset profiles, it may be useful for tracking purposes as the profile is used for risk assessment and other purposes, particularly as an information asset changes.

Further, it may be necessary to investigate or know the history of an information asset profile as the asset matures. By specifying when the asset was profiled and by whom, a higher continuity is ensured. For example, enterprise managers may want to track all instances of an IAP for a specific asset to assess significant changes in ownership, custodianship, or value over the life of the asset within the enterprise.

### Important Tips

Documenting the IAP creation date and naming those who performed the IAP is not a trivial activity. The historical value of an asset may surpass the actual value of an asset as a commodity over time. For example, the ability to track an asset's value in importance from the asset's inception to maturity to decline may help in devising protection mechanisms or serve as a predictor for similar information assets in the future. Therefore it is important to capture the date of the IAP creation, the version information, and the names of personnel who create the IAP. Some important items are

- recording not only the names of personnel but the roles (e.g., Director of Financial Services and asset X's owner) they currently occupy in the organization and their contact information. Whenever possible, the owner of the asset and other relevant stakeholders should be included in this process. This helps to ensure the acceptance of the output.

- creating a version number for the IAP that follows a standard, enterprise-wide convention. The main purpose of the version number is to capture the order, change history, and version control information.
- cross-referencing the version or date information by making reference to the IAP that has been updated or superseded by the current version

### Performing the Activity

The following steps are required to complete this activity.

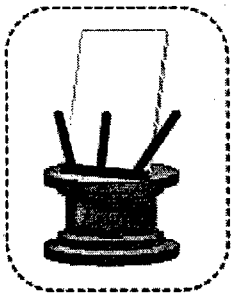
1. Record the names, relevant titles/roles/positions, and contact information for each of the individuals who are creating this IAP.
2. Record the date on which the profile is created.
3. Record the version of the IAP.

### Example

The following example uses a fictional information asset of patient medical records for a fictional hospital. The example will be used throughout this section as a continuous illustration of the IAP process as each activity is performed.

| **Information Asset Profile** | | | | |
|---|---|---|---|---|
| **Information Asset Name** | Patient Medical Record | | | |
| **Date Created** | Sept. 15, 2006 | **Version #** | HMC_A01_030915 *[No prior IAP performed for this asset]* | |
| **Profile Creators** | Bob Vienna, Medical Technician, Endocrinology Dept. | Charlotte Evans, RN, Outpatient Surgical Ward "A" | Doug Stemple, System Analyst, Medical System Support Dept. | Ester Johnson, Director of Medical Records, Records Management Dept. |

## Activity 2 - Define the Information Asset



### Purpose

The purpose of this step is to characterize an information asset. Before any type of analysis activity (e.g., risk assessment) can be performed on an information asset, the organization must understand and agree upon what an information asset contains.

### Concepts

The level of detail that is captured should assist in

- defining the content of an asset and its boundaries
- determining ownership of the asset
- determining the value (monetary or otherwise) of the asset
- determining the security requirements of the asset

The depth to which an asset must be defined depends largely on the organization and how the information asset profile will be used. Keep in mind that being too deliberate in defining information assets may not enhance the ability to assess these assets for risk or to develop a protection strategy. Thus, using good judgment and being consistent in defining assets can reduce the issues related to the many combinations and permutations of combined (complex) information assets.

Some information assets are highly tangible. For example, if a patient's medical records exist only on paper, the "contents" of this information asset are visible. In other cases, an information asset may not be as visible. This may be the case of an information asset such as a "vendor database" or "customer database" that exists only in electronic form. In these cases, it takes more examination of what is contained in the vendor database to truly define the asset.

The definition of the information asset should strive to satisfy these requirements at a minimum:

- consistency (the definition does not change over short periods of time or in different settings)
- clarity (the definition lacks ambiguity and vagueness and is not subject to interpretation)

- universal understandability (the definition transcends different lexicons and technologies)
- acceptance (the definition is acceptable to all who have a need to know)
- physicality (the definition is clear as to how the asset is physically instantiated—i.e., electronically or on paper, microfiche, etc.)

Considering these qualities will provide an adequate definition that can be used throughout the organization. (Additional background concepts are provided in Section 2.2.)

### Important Tips

For an initial definition of an information asset, it is generally acceptable to use the highest level of description that accurately represents the boundaries of an asset and its contents. For example, in describing the vendor database, it may be perfectly acceptable to state "all of the tables, fields, and data elements in the vendor database that support our integrated financial system." However, this will not be the case in some instances. For example, "medical records" can be a vague definition of an asset. If instead the asset is described by its component parts—patient information, diagnosis information, and treatment information—there is more clarity, consistency, etc.

When developing an information asset description, it may be advantageous to initially provide more data than less and to shape and sharpen the definition as more information profiling activities are performed. However, too much detail can overwhelm those who rely on the definition.

Additional tips:

- Be aware that the process of defining the information asset may result in the definition of one or more assets. Delving into the detail of an information asset may result in a better delineation of the asset into two distinct logical assets, even though the asset may be physically stored, transported, or processed on a regular basis as a single asset.
- Stay away from technical conventions when describing information assets, and only use them when they enhance (or are essential to) the definition. For example, naming all of the fields or tables in the vendor database to define the "vendor" asset may be overkill. It may provide comfort that the boundaries have been tightly defined but may provide no advantage in using the asset for risk assessment later on.
- Be sure to define both electronic and paper assets. Sometimes an information asset exists in either or both forms. This should be captured in the description because it will eventually affect risk mitigation planning to secure the assets.
- Involve the owner of the asset and other relevant stakeholders in the definition process. This will ensure the accuracy and consistency of the definition and the acceptance of stakeholders. In some cases the owner will not be able to be determined until after the asset is defined. In these cases, the definition of the information asset should be reviewed with the owner after the owner is identified in Activity 3 to ensure agreement.

- In some cases it may make sense to include in the description specific information that is excluded from the asset. It is possible that an asset is easier to bound by explaining what is not included as well as what is included. The purpose is to ensure that the reader understands the contents and the boundaries of the information asset. (Please note that exclusion information was not included in the example because its description sufficiently bounds the asset for the audience that is likely to use the profile without it.)
- In addition to including information about content that is excluded from an asset, it is often useful to include notes explaining why decisions were made about bounding the asset. The purpose of these notes is to provide insight to others looking at the asset profile.

### Performing the Activity

The following steps are required to complete this activity.

1. Examine the information asset and develop a description.
2. Record the description on the information asset profile worksheet. (Remember: if two or more assets are defined, describe each on a separate information asset profile form.)
3. Resolve any issues regarding the description detail before you proceed.
4. Use the description from Step 2, above, and then record an appropriate information asset name on the information asset profile worksheet.

### Example

After getting started with the profiling process, the group developing the profile for the medical records asset determined that the asset appeared in both electronic and in paper forms. Their first impression was that the security requirements and descriptions of these assets would be similar, and they decided to move the process forward treating the electronic and paper records as the same asset.

Further examination of the records showed there was information that was in the electronic record that was not present in the paper records and there was information in the paper records that was not present in the electronic records. In addition, the group revealed that there were different regulations on how paper medical records and electronic medical records were to be treated. At this point a determination was made to treat the paper and electronic records as separate assets.

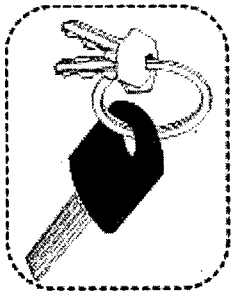
This example will only carry through with the electronic medical records.

| Information Asset Description | This asset is composed of the collection of all data, records, and information in electronic format necessary to render treatment to a patient, including (historical)<br>▪ patient background, demographic, and medical profile (mostly information provided by the patient, including name, address, DOB, ID, emergency contact, allergy, surgical history, etc.)<br>▪ laboratory and diagnostic testing results and records<br>▪ doctor/nurse/medical technician notes on stats, diagnosis, treatment, and/or referral<br>▪ specialist notes on treatment, recommendations, and progress of treatment<br>▪ patient insurance and billing information – only information that is medically relevant to diagnosis, treatment, or referral (insurance/payment restrictions, etc.)<br><br>Note: Patient medical records also exist in physical paper and microfiche forms as well as electronic media formats. This asset profile is only concerned with the records in electronic formats. |
|---|---|

After determining that the information asset described was used for the sole purpose of rendering medical treatment to a patient, it was agreed that the description for Patient Medical Records does *not* include the following information:

- Payment and/or billing history and status, including other specific billing information, with the exception of information that must be known to the medical provider to render treatment. For example, defaults/debts or payments outstanding, payment history, and insurance policy numbers, etc. are not necessary for treatment and are not mandatory information for this asset. However, insurance carrier and service-hold status (e.g., a patient's account status allows for only emergency medical treatment because of payment debt or defaults outstanding) may be indicated in the asset's records.

## Activity 3 - Identify the Asset Owner



### Purpose

The purpose of this activity is to identify and document the owner of the information asset. This activity is important because the owner should work with the individual or group performing the IAP in the remainder of the activities.

### Concepts

Ownership of information assets is often confounding for an organization. Identifying ownership is one of the most important activities in effective security and risk management of information assets that an organization can perform. Many organizations have never taken an accurate and complete inventory of their information assets. The failure to identify asset owners is one of the primary reasons why information security management is often ineffective in organizations.

The owner of an information asset should be an organizational stakeholder (or organizational unit) that is responsible and accountable for

- describing the information asset (see Activity 2, above)
- defining the security requirements of the information asset (see Activity 5, below)
- communicating the security requirements of the information asset to all custodians and users
- ensuring that the security requirements are met (via regular monitoring)
- designing an appropriate protection strategy to protect the information asset
- determining risks to the information asset
- developing strategies to mitigate risks to the information asset

The owner of an information asset may have an organizational or a legal responsibility for ensuring the asset's viability and survivability.

### Important Tips

In the process of defining an asset, it may be realized that the asset has more than one owner. Often, this is an indication that the asset being defined is, in actuality, more than one asset. If this is the case, an information asset profile should be created for each asset and ownership should be documented accordingly.

Remember that in many organizations owners are often simply assumed to be those who manage the asset's containers, and thus ownership is "assigned" to those who take custody of the asset from a technical standpoint (i.e., system administrators, database administrators, and IT staff in general).

Ownership can also be confused with data creation or origination. The creators of data or information are not necessarily the owners of information assets. Ownership is often assigned in organizations without regard to who (or what system, etc.) created the information or where it originated (internally, with an outside vendor, etc.). These issues are often irrelevant as long as ownership is established and the stakeholder who has accepted ownership also has the responsibility and authority to perform ownership duties.

In capturing ownership information, the focus should be on the role or position within the organization that has ownership of an information asset and not a specific person. In many organizations the people in specific positions change much more frequently than the positions themselves.

### Performing the Activity

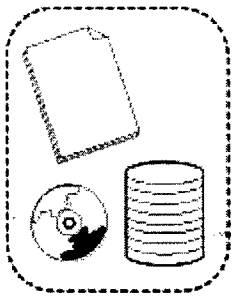
The following steps are required to complete this activity.

1. Record the owner of the information asset being profiled. The owner should be a role/position within the organization.
2. For each owner, record contact information for the person currently acting in the role as owner.

### Example

| | |
|---|---|
| **Information Asset Owner(s)** | Division Chief and Senior Director, Records Management Dept.<br>[As of 030915: Tobi MacGillicutty, Rm. G910, ext. 553] |

## Activity 4 - Identify Containers



### Purpose

The purpose of this step is to capture a list of all of the containers on which an information asset is stored, transported, or processed and the associated list of the managers of those containers. This step can be done in parallel with Activity 3, as there are no dependencies between the two activities.

### Concepts

In an information security risk assessment, the identification of key containers is essential to identifying the risks to the information asset itself. An information asset is protected through controls implemented at the container level. The level of protection provided by the controls is directly related to how well they implement the security requirements of the information assets. Any risks to the containers on which the information asset lives are inherited by the information assets.

This activity efficiently defines the boundaries of the environment that must be examined for risk. It also describes the custodial relationships that must be understood for successfully communicating security requirements and for designing effective security controls. This is especially important in resolving some of the previously described dilemmas of data.

The containers that are captured are broken down into four categories:

- systems and applications
- hardware
- people
- other containers

In addition to capturing the list of containers, the managers of those containers also need to be captured. The manager of the container takes custodianship of an information asset and may be required to implement the security requirements of the information asset. It may be necessary to talk with the container managers during the risk assessment process to gather additional information.

### Important Tips

As with the asset definition, the level of detail necessary to be captured in this activity is highly dependent on the organization and on how the asset profiles will be used. In a small organization with only a few systems, it may be practical to consider each container individually. In organizations where there are large classes of similar systems managed by an IT department or departments, it may make sense to simply collect the class of container to be considered.

Some basic questions to consider when enumerating containers:

- What information systems or applications use or process this information asset?
- On what hardware platforms might the information asset be found?
- What people have access to the information asset? Can these people be categorized into groups?
- Are any automated processes reliant on the information asset?
- What media types are used to store the information asset?
- Is the information asset often printed, who would print it, and where are printed copies stored?
- Does the information asset ever enter the possession of a customer or partner?
- Are backups or offsite storage of the information asset contracted to a third-party organization?
- Are there any internal or external spaces where the information asset might be stored in physical form (paper, tape, CD-ROM, etc.)?

The information captured on the container manager should focus on the role or position within the organization that has ownership of the information asset and not a specific person, unless a specific person acts as a container for the information asset.

### Performing the Activity

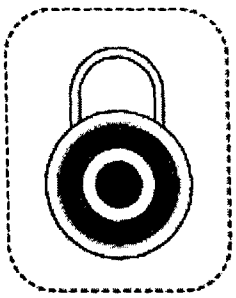
The following steps are required to complete this activity.

1. For each category of container, record the name of all the containers on which the information asset is stored, transported, or processed.
2. For each container, record the owner of that container. The owner should usually be a recorded as a role/position within the organization and not a specific person.

**Example**

| Key Containers for Information Asset | |
|---|---|
| **(1) Systems and Applications** | |
| ❑ Application systems | Medical Records Database System (MRD Manager)<br>Bedside Treatment Systems (BTS Manager)<br>Physician Desktop Systems (PDS Manager) |
| ❑ Operating system | |
| ❑ Other systems and applications | |
| **(2) Hardware** | |
| ❑ Servers and other hardware | |
| ❑ Networks and network segments | Office Network (Hospital Network Manager)<br>Treatment Network (Hospital Network Manager) |
| ❑ Personal computers and other hardware | |
| **(3) People** | |
| ❑ Subject matter experts/business units | |
| ❑ Technical personnel | |
| ❑ Other employees | |
| **(4) Other Containers** | |
| ❑ Physical storage locations | Backup tapes (offsite at ALLsafe Storage, Inc.) |
| ❑ Paper/paper files | |
| ❑ Personal storage (desks, home) and other locations | Physician PDAs (individual physicians)<br>Physician laptops (individual physicians) |

## Activity 5 - Identify Security Requirements



### Purpose

The purpose of this step is to capture the specific security requirements of the information asset.

### Concepts

The security requirements of an information asset are generally defined across the dimensions of confidentiality, integrity, and availability. These dimensions are referred to as security objectives by the Federal Information Systems Management Act of 2002 and are defined as follows:

- *Confidentiality* is "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information ..." [44 U.S.C., Sec. 3542]
- *Integrity* is "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information ..." [44 U.S.C., Sec. 3542]
- *Availability* is "ensuring timely and reliable access to and use of information ..." [44 U.S.C., Sec. 3542]

It is very important that the security requirements of an information asset be accurately specified. If an owner cannot detail the security requirements for an asset, then the owner cannot expect that anyone to whom he or she grants custodial control of the asset will appropriately protect it.

### Important Tips

- Recognize that the information may be subject to external agreements or licensing terms that dictate additional security requirements. Information assets often include data from other information assets or from external parties. The use of this data is often covered by acceptable use policies and licensing agreements that describe who may use the data, when the data can be used, or what can be done with the data. Make sure that any of these additional requirements is included in the security requirements and use the "NOTES" section to describe where the requirements originated.
- Recognize that the information may be subject to laws or regulations that also dictate additional security requirements. Any additional security requirements specified by a law or regulation should be included, and the "NOTES" section should be used to describe where the requirement originated.
- As with most other steps, the use of roles is preferred to the use of individuals when describing requirements.
- Requirements should be stated as explicitly as possible.
- This is another step where examination of the asset may result in the determination that the information asset is actually two separate assets.
- The information asset owner is responsible for specifying the security requirements for an information asset. In many organizations, the owner will delegate the responsibility for this to the team developing information asset profiles. When this is the case, the team should ensure that the owner is involved.
- The stakeholders of an asset are an excellent source of security requirements and are also excellent for checking draft security requirements.

### Performing the Activity

Record the confidentiality, integrity, and availability requirements for the information asset.

**Example**

| Security Requirements | Confidentiality |
|---|---|
| | All information in an Electronic Patient Medical Record is considered sensitive and operationally significant to the hospital, care provider, and patient regardless of its current location.<br><br>Patients require this information to remain confidential to authorized hospital personnel with a strict need-to-know for their care during the processing, transmission, or storage of this information. |
| | NOTES:<br>The information in the electronic medical record is protected by HIPAA regulations, which give patients authority to determine who has access to their records. |

| | Integrity |
|---|---|
| | The hospital staff requires this information to be accurate, correct, and unmodified—unless provided, recorded, or updated by authorized hospital staff or the primary care provider.<br><br>State regulations require that no information may ever be removed from a medical record unless specifically directed by the patient.<br><br>Only authorized laboratory staff may create or update information concerning laboratory reports.<br><br>Only authorized treatment staff may update or create patient notes and treatment plans.<br><br>Patient background and billing information is to be provided by and approved by the patient. Only authorized hospital data entry staff may create or modify patient background or billing information. The patient must be notified of and authorize changes to background and billing information. |
| | NOTES:<br>Accurate treatment is dependent on the integrity of the information in the electronic medical record.<br><br>State Law 1443 Section 2AC requires that information may only be removed from an electronic medical record when authorized by a patient.<br><br>HIPAA grants patients control of who can change information in their medical treatment records. |

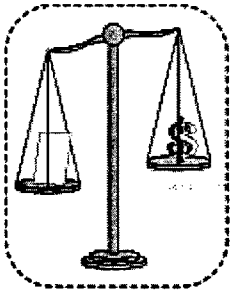
| | Availability |
|---|---|
| | This information must be available to the hospital treatment staff to make treatment decisions for patients on a 24 hour, 7 day, 365 day/year basis.<br><br>This information must be available to the Accounts Receivable department on a 9-5 basis 5 days per week to produce billing statements.<br><br>This information must be made available to external auditors from the state health regulator's office within 24 hours of an audit notice. |
| | NOTES:<br>State Law 1443 Section 2AD requires that patient medical records can be audited for due care by the state health regulator's office. |

The hospital staff working on developing the profile considered breaking the electronic medical record into four separate assets:

- patient background information
- patient billing information
- patient treatment information
- patient laboratory information

Each of these categories of information within the electronic medical record had a set of clearly distinguishable security requirements. However, in this case the information was almost always stored, transported, and processed together, and most users in the hospital viewed the record as a single entity.

## Activity 6 - Determine the Information Asset Valuation



### Purpose

Before the risks to an information asset can be assessed, the tangible and intangible value of the asset must be known.

### Concepts

The owner of the information asset and its stakeholders should determine the value of the information asset to the enterprise or business unit. The contribution of the asset to the owner's goal achievement (or the potential to impede goal achievement) should be reflected in the valuation. Determining the value is an attempt to capture how important this information is to the organization, mainly the value derived from its use but also considering the impact of its loss or unavailability.

Valuing information assets has proven to be very hard for many organizations. Information assets are not often carried on the books as capital investments, so determining a monetary equivalent is not always straightforward. Often the value of an information asset is found in the process it supports and not in the information itself. One way to consider the value of an asset is to look at the potential impact on the organization if something were to happen to it. Every organization will need to determine for itself the appropriate type of valuation.

In the federal space, a significant amount of guidance has been issued to help federal government agencies determine a valuation for their information assets. FIPS Publication 199 [NIST 04a] and the NIST Special Publication 800-60 volumes [NIST 04b] provide explicit guidance. An asset's value is determined by looking at the potential impact on the organization if the security of the asset were to be compromised. Information is first classified by type (public relations information, for example). Then for each type of information the potential impact is rated on a simple high, medium, or low value for each security objective (confidentiality, integrity, and availability).

An asset's value is determined by looking at the potential impact on the organization if the security of the information asset were to be compromised. Information is first classified by type (public relations information, for example). Then for each type of information the potential impact is rated on a simple high, medium, or low value for each security objective

(confidentiality, integrity, and availability). The table below, taken from the FIPS Publication 199 guidance, provides a simple example of how the potential impact is rated across each of the security objectives.

*Table 1: Potential Impact Definitions for Security Objectives*

| | Potential Impact | | |
|---|---|---|---|
| **Security Objective** | **Low** | **Moderate** | **High** |
| **Confidentiality** | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity** | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability** | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

## Important Tips

- Always consider the costs to the organization if the security requirements of an asset are violated.

- Talk to the owners and stakeholders of an information asset and determine what it produces or what processes rely on it. The more important the output or process, the more significant the information asset.
- Consider external impacts, such as legislation, regulation, and reputation, when developing your valuation.
- The ultimate goal of a valuation is to be able to do a cost benefit tradeoff analysis. The valuation should include information to allow decision makers to make informed choices.
- Remember that this step is not concerned with an assessment of risk to the asset. The likelihood of an impact should not be considered.
- An organization should use the method that it believes will provide the most useful valuation of an information asset.

### Performing the Activity

Determine the value of an information asset and then capture this information on the information asset profile worksheet.

### Example

| | |
|---|---|
| **Information Asset Valuation** | The Patient Medical Record is considered essential for operation of the hospital and for the success of the day-to-day mission of providing quality care to our clients, whether we provide laboratory, diagnostic, therapeutic, in/out-patient treatment, emergency, surgical, or other health-related services. The value, as a function of loss, harm, or costs due to the inappropriate or erroneous use (whether accidental or deliberate), modification, loss, theft, destruction, or unavailability, carries potential for impacts that could be catastrophic. For example:<br>▪ Failure to secure a medical record to authorized parties could cause fines and legal suits from patients, state officials, and the government.<br>▪ The loss or unauthorized modification of a medical record, in part or in full, could cause operational and quality problems in rendering care, resulting in loss of life, staff effectiveness and efficiency, and other problems. |

# Appendix B IAP Worksheets

| Information Asset Profile | | | | |
|---|---|---|---|---|
| **Information Asset Name** | | | | |
| **Date Created** | | **Version #** | | |
| **Profile Creators** | | | | |
| **Information Asset Description** | | | | |
| **Information Asset Owner(s)** | | | | |

| Information Asset Profile | | | |
|---|---|---|---|
| **Information Asset Name** | | | |
| **Date Created** | | **Version #** | |

| Key Containers for Information Asset | |
|---|---|
| **(1) Systems and Applications** | |
| ❑ Application systems | |
| ❑ Operating system | |
| ❑ Other systems and applications | |
| **(2) Hardware** | |
| ❑ Servers and other hardware | |
| ❑ Networks and network segments | |
| ❑ Personal computers and other hardware | |
| **(3) People** | |
| ❑ Subject matter experts/business units | |
| ❑ Technical personnel | |
| ❑ Other employees | |
| **(4) Other Containers** | |
| ❑ Physical storage locations | |
| ❑ Paper/paper files | |
| ❑ Personal storage (desks, home) and other locations | |

| Information Asset Profile | | | |
|---|---|---|---|
| **Information Asset Name** | | | |
| **Date Created** | | **Version #** | |
| **Security Requirements** | **Confidentiality** | | |
| | | | |
| | NOTES: | | |
| | **Integrity** | | |
| | | | |
| | NOTES: | | |
| | **Availability** | | |
| | | | |
| | NOTES: | | |

| Information Asset Profile | | | |
|---|---|---|---|
| **Information Asset Name** | | | |
| **Date Created** | | **Version #** | |
| **Information Asset Valuation** | | | |

# References

*URLs are valid as of the publication date of this document.*


**[Alberts 01]** Alberts, Christopher J. & Dorofee, Audrey J. *OCTAVE Criteria V2.0* (CMU/SEI-2001-TR-016, ADA3399229). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. http://www.sei.cmu.edu/publications/documents/01.reports/01tr016.html.

**[Caralli 04]** Caralli, Richard A. *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* (CMU/SEI-2004-TR-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/publications/documents/04.reports/04tr010.html.

**[NIST 04a]** National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2004. http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

**[NIST 04b]** National Institute of Standards and Technology. *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories and Volume II: Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories (NIST Special Publication 800-60)*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2004. http://csrc.nist.gov/publications/nistpubs/.

**[Stoneburner 02]** Stoneburner, Gary; Goguen, Alice; & Feringa, Alexis. *Risk Management Guide for Information Technology Systems (NIST Special Publication 800-30)*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

**[Webster 04]** Merriam-Webster, Inc. *Merriam-Webster Online Dictionary.* http://www.m-w.com/ (2005).

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. AGENCY USE ONLY | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| (Leave Blank) | June 2005 | Final |

| 4. TITLE AND SUBTITLE | 5. FUNDING NUMBERS |
|---|---|
| Information Asset Profiling | F19628-00-C-0003 |

6. AUTHOR(S)

James F. Stevens

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|
| Software Engineering Institute<br>Carnegie Mellon University<br>Pittsburgh, PA 15213 | CMU/SEI-2005-TN-021 |

| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER |
|---|---|
| HQ ESC/XPK<br>5 Eglin Street<br>Hanscom AFB, MA 01731-2116 | |

11. SUPPLEMENTARY NOTES

| 12A DISTRIBUTION/AVAILABILITY STATEMENT | 12B DISTRIBUTION CODE |
|---|---|
| Unclassified/Unlimited, DTIC, NTIS | |

13. ABSTRACT (MAXIMUM 200 WORDS)

The steadily increasing technical and environmental complexity of today's globally networked economy presents many obstacles to organizations as they attempt to protect their information assets. Information assets are constantly processed and combined to form new information assets. The line between ownership and custodianship of information assets blurs as information freely flows throughout an organization and often crosses outside organizational boundaries to other entities such as partners, customers, and suppliers. The CERT Survivable Enterprise Management group at the Software Engineering Institute developed the Information Asset Profiling (IAP) process as a tool to help organizations begin to address these security challenges.

The authors describe IAP, a documented and repeatable process for developing consistent asset profiles. They also explain how the development of an information asset inventory using the IAP process provides a strong basis for organizations to begin to identify and address their information security needs.

| 14. SUBJECT TERMS | 15. NUMBER OF PAGES |
|---|---|
| information assets, information security, security requirements, risk management | 61 |

16. PRICE CODE

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UL |